



September 15, 2014

About STELLARWIND and other mysterious classification markings

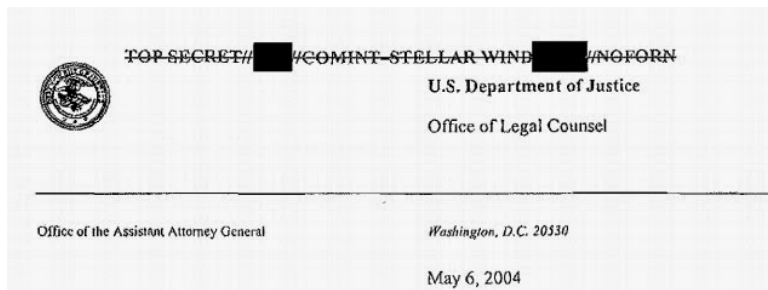
(Updated: September 15, 2014)

Last week, on September 6, the US Justice Department **released** a declassified version of a 2004 memorandum about the **STELLARWIND** program.

The **memorandum (pdf)** is about the legality of STELLARWIND, which was a program under which NSA was authorized to collect content and metadata without the warrants that were needed previously.

Here we will not discuss the STELLARWIND program itself, but take a close look at the STELLARWIND classification marking, which causes some confusion. Also we learn about the existence of mysterious compartments that point to some highly sensitive but yet undisclosed interception programs.

> See also: [The US Classification System](#)



Classification marking of the 2004 DoJ memorandum about STELLARWIND

The redacted markings

The first thing we see is that two portions of the classification marking have been blacked out:

Welcome to this weblog about Top Level Telecommunications!

Here you can read about:

- Signals Intelligence (SIGINT),
 - Communications Security (COMSEC),
 - Information Classification,
- and also about the equipment, from past and present, which make that civilian and military leaders can communicate in order to fulfill their duties.

The main focus will be on the United States and its National Security Agency (NSA), but attention will also be paid to other countries and subjects.

Any comments, additions, corrections, questions or suggestions will be very appreciated! There's no login or registration required for commenting.



twitter.com/electrospaces



[info \(at\) electrospaces.net](mailto:info@electrospaces.net)

PGP Public Key ID: **FD9FD4E6**

The postings on this weblog are updated frequently as new information about the NSA is still being revealed. Therefore, revisit this weblog and check the articles for updates!

Recent Posts

[About STELLARWIND and other mysterious classification markings](#)

[NSA's foreign partnerships](#)

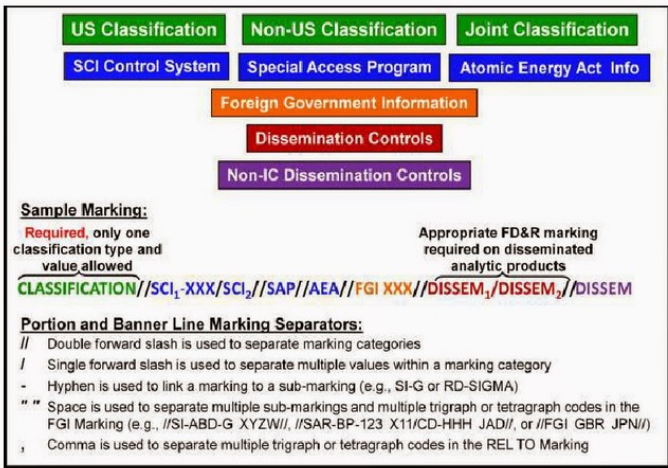
[Another "red phone" for the Israeli prime minister](#)

1. The redacted space between two double slashes

This is very strange, because according to the official classification manuals, there cannot be something between two double slashes in that position (see the chart below). The classification level (in this case: Top Secret) has to be followed by the Sensitive Compartmented Information (SCI) control system (here: COMINT).

But as the US classification system is very complex, there are often minor mistakes in such classification lines. If we assume there was a mistake made here too, then the first term that has been blacked out could be another SCI compartment, which had to be followed by just a single slash (for example HCS for HUMINT Control System would fit the redacted space, although that marking itself isn't classified).

If there was no mistake, however, and the double slash is actually correct, then it would be a complete new category which isn't in the (public) classification manuals. This reminds of the UMBRA marking, which also appeared unexpectedly between double slashes in a classification line.



Overview of the categories and formatting for the US classification and control markings
From the Intelligence Community Classification Manual 6.0 from December 2013
(click to enlarge)

2. The redacted space directly after STELLARWIND

The second redaction starts right after the last letter of "STELLARWIND", thereby carefully hiding the category of the redacted marking, which is determined by how it is separated from the previous term. This could be by a slash, a double slash, a hyphen or a space, each indicating a different level.

In this case, the most likely option is that "STELLARWIND" is followed by a hyphen, which indicates the next term is another compartment under the COMINT control system, equal to STELLARWIND.

Classification manuals say there are undisclosed COMINT compartments which have identifiers consisting of three alphabetical characters. This would fit the redacted space as it would read like: "COMINT-STELLARWIND-ABC".

This undisclosed compartment probably also figured in some other declassified documents, where it sometimes seems to be accompanied by a sub-compartment which is identified by three numeric characters, like for example in this and this declaration where the marking could read like "COMINT-ABC 678":

What if Google was an intelligence agency?

New phones aboard Air Force One

Document shows that it was not NSA, but FBI that monitored 5 Americans

NSA still uses the UMBRA compartment for highly sensitive intercepts

The National Security Agency in 2002

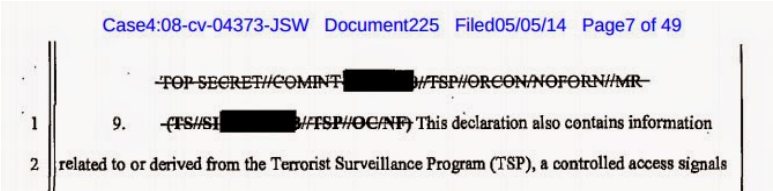
Snowden-documents show no evidence for global mass surveillance

"It's actually straight up interesting but also weird how weirdly, wonderfully detailed this blog about hyper secure communications is."
— Gizmodo.com

Pages
Home
INDEX
Links
Abbreviations and Acronyms
NSA Nicknames and Codewords
NSA's organizational designations
NSA Glossary
The US classification system
SIGINT Activity Designators (SIGADs)
GCHQ Nicknames and Codewords
Telephony & Internet Abbreviations

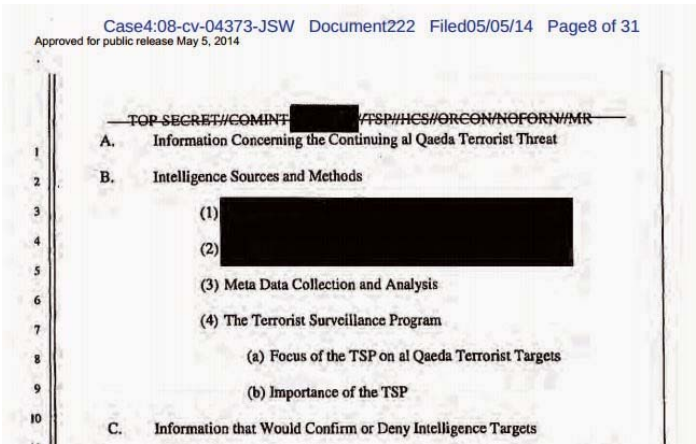
Total Pageviews
572,589

Popular Posts
How Obama's BlackBerry got secured
New phones aboard Air Force One
DRTBOX and the DRT surveillance systems
New slides about NSA collection programs
The US Classification System
Some numbers about NSA's data collection
New insights into the PRISM program



Classified declaration of NSA director Alexander, April 20, 2007.

Looking at what was redacted in portions of both documents which were marked with this mysterious compartment, it seems that it's about at least two highly sensitive intelligence sources and methods. For example, pages 31-32 of this [declaration \(pdf\)](#) suggest that this might be obtaining metadata from specific telecom companies and search them for members or agents of particular target groups.



Classified declaration of Director of National Intelligence John Negroponte, May 12, 2006
TSP = Terrorist Surveillance Program; HCS = HUMINT Control System
Note that TSP and HCS are also between double slashes
(click to open the full document in pdf)

Markings with the mysterious undisclosed COMINT compartments weren't found on any of the Snowden-documents, but only on those that were declassified by the government, so it seems that Snowden had no access to information protected by these particular compartments.

The marking TSP (for Terrorist Surveillance Program), which is in some of the examples shown above, was used instead of STELLARWIND in briefing materials and documents intended for external audiences, such as Congress and the courts.

The STELLARWIND marking

So far, we looked at the two parts of the classification marking that were blacked out. But now we also have to look at the STELLARWIND marking itself, which wasn't redacted, but still causes confusion.

The classification marking of the 2004 memorandum of the Justice Department says "COMINT-STELLAR WIND" and according to the official formatting rules, this means that STELLARWIND would be part of the COMINT control system.

Note that the same memorandum had already been declassified upon a FOIA request by the ACLU in 2011, but in [that version \(pdf\)](#) the codeword STELLARWIND was still blacked out from the whole document. Both documents are compared [here](#).

Labels

Air Force One (1) Apple (1) BlackBerry (1) Boeing (1) BoundlessInformant (7) Brazil (1) Britain (1) Canada (1) Classification (6) CSEC (2) GCHQ (2) General Dynamics (1) Germany (4) Gold Phone (1) GSM (2) Hotline (4) ISAF (1) Israel (2) IST (2) Kremlin (1) Metadata (3) Netherlands (4) North Korea (1) NSA (28) NSA Partnerships (4) Obama (3) POTUS (7) PRISM (7) Red Phone (5) Russia (1) Situation Room (1) STE (3) STU-II (1) STU-III (1) UMTS (2) USA (2) USSR (2) Vatican (1) VolP (1) White House (3) Wireless (6)

Search This Blog

Search

Blog Archive

▼ 2014 (23)

▼ September (2)

About STELLARWIND and other mysterious classificat...

NSA's Foreign Partnerships

► August (2)

► July (4)

► June (2)

► May (2)

► April (1)

► March (3)

► February (5)

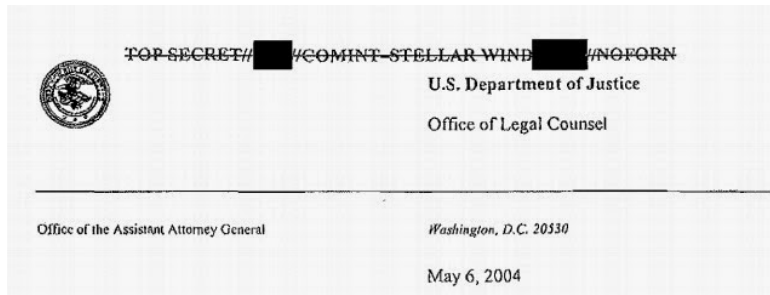
► January (2)

► 2013 (33)

► 2012 (10)

US Red Phones

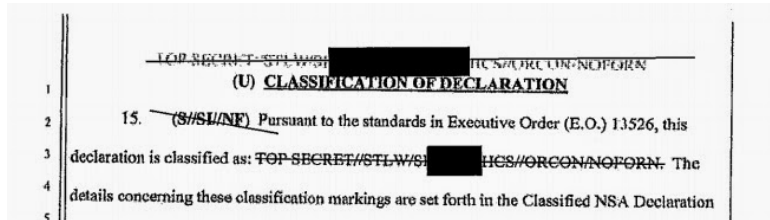
Sequence of the real Red Phones, not for the Washington-Moscow Hotline, but for the US Defense Red Switch Network (DRSN). The phones shown here were in use from the early eighties up to the present day and most of them



Classification marking of the 2004 DoJ memorandum about STELLARWIND

As COMINT is a control system for communications intercepts or Signals Intelligence, this seems to make sense. But what is confusing, is that the internal 2009 NSA [classification guide \(pdf\)](#) for the STELLARWIND program, which was disclosed by Edward Snowden, says something different.

Initially this guide calls STELLARWIND a "special compartment", but from the marking rules it becomes clear that it is treated as an SCI control system. Accordingly, the prescribed abbreviated marking reads: "TOP SECRET // STLW / SI // ORCON / NOFORN". In this way we can see STELLARWIND in the classification line of the following document:



Classification marking of a 2013 [classified declaration \(pdf\)](#) of DNI James Clapper
which was declassified on May 6, 2014
(click to enlarge)

In this document and also in a similar [declaration \(pdf\)](#) from 2013, the reason for the STELLARWIND classification is explained as follows:

"This declaration also contains information related to or derived from the STELLARWIND program, a controlled access signals intelligence program under presidential authorization in response to the attacks of September 11, 2001. In this declaration, information pertaining to the STELLARWIND program is denoted with the special marking "STLW" and requires more restrictive handling."

STELLARWIND is also being treated as a control system in the [2009 draft report](#) about this program written by the NSA Inspector General, although its classification line is also somewhat sloppy: there are double slashes between STLW and COMINT (should just be a single one), and only a single one between COMINT and ORCON (where there should have been double slashes as both are from different categories):



Classification marking of the 2009 report about

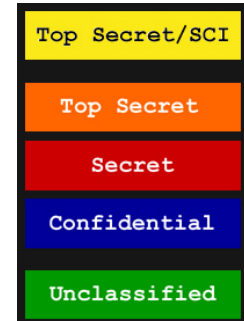
were made by ElectroSpace Systems Inc. They will be discussed on this weblog later.

For the record, you see:

- ElectroSpace MLP-1
- ElectroSpace MLP-1A (since 1983)
- ElectroSpace MLP-2
- Raytheon IST (since 1992)
- Telecore IST-2 (since 2003)

US Classification Levels

Color codes for the [classification levels](#) used by the government and the armed forces of the United States:



These color codes are used to mark the classification level of (digital) documents and files and also of the communication devices used for their transmission.

Subscribe to this weblog!

- Posts
- Comments

Hotlinks

- The Dutch virtual [Crypto Museum](#)
- Website about [Crypto Machines](#)
- Intelligence expert [Matthew Aid](#)
- Bruce [Schneier on Security](#)
- Steven Aftergood's [Secrecy News](#)
- The weblog [Empty Wheel](#)
- Stewart Baker's [Skating on Stilts](#)
- Marc Ambinder's [The Compass](#)
- Leaked documents: [IC Off the record](#)
- Glenn Greenwald's [The Intercept](#)
- Der Spiegel's [53 NSA-documents](#)
- The [NSA Observer](#)
- The [Cryptome](#)
- > [Many more links](#)

STELLARWIND by the NSA Inspector General
(click to read the full document)

Throughout this document, the portion markings are also not always consistent. Most of them are "TS//SI//STLW//NF", but one or two times "TS//SI-STLW//NF". But as this report is a draft, it's possible that these things have been corrected in the final version, which hasn't been disclosed or declassified yet.

The 2009 Inspector General report about STELLARWIND was one of the first documents from the Snowden-leaks to be **published**, and it still is one of the most informative and detailed pieces about the development of NSA's interception efforts since 9/11.

Conclusion

In the end, it doesn't make much difference whether STELLARWIND is a control system on its own, or a sub-system of COMINT, but it is remarkable that for such an important program, the people involved apparently also weren't clear about it's exact status and how to put it in the right place of a classification line.

More important though is that the declassified documents show that besides the STELLARWIND program, there's at least one COMINT-compartment with at least one sub-compartment that protect similar or related NSA collection efforts which are considered even more sensitive, but about which we can only speculate.

Geplaatst door **P/K** op **01:05**

 Recommend this on Google

Labels: **Classification**

3 comments:

 **rsesek** said...

My hypothesis is that STELLARWIND started as an highly classified COMINT compartment, which is what the early documents show. The entire STLW system was set up under emergency legal powers after 9/11, so the legal framework for the collection was not long-lasting. But then the Executive Branch got FISA amended (a couple of times...) to grant power to collect in a STLW-like way. The FISA-based legal framework is somewhat different than what STLW was originally set up to do, and the IG report shows that STLW collected data in some legally questionable ways. I think that after FISA was updated, STELLARWIND was made a control system to protect and isolate the data collected under that temporary, emergency authority, which is why the classification guides are so explicit about not removing information from the control system. Data collected under the authority is collected in an SI compartment, just like STLW was originally.

Also, one note: HCS (and other control system markings) are sometimes redacted so that a document is not associated with an agency, not because the marking itself is classified.

September 16, 2014 at 5:34 PM

Anonymous said...

Sorry for my lack of knowledge on this site, but I don't know where to post updates. In your GCHQ list of abbreviations you have JARIC. This stands for Joint Air Reconnaissance Intelligence Cell. This uses UK air assets to record imagery, analyse and disseminate product.

September 19, 2014 at 7:16 PM



P/K said...

Thank you for mentioning this! You can post comments below every article on this website. I will update the GCHQ listing accordingly.

September 19, 2014 at 8:45 PM

Contact

For questions, suggestions and other remarks about this weblog in general or any related issues, please use the following e-mail address: **info (at) electrospace.net**

For sending an encrypted e-mail message, you can use the PGP Public Key under this ID: **FD9FD4E6**

You can also communicate through Twitter: **@electrospace** or XMPP/Jabber chat by using the address **electrospace (at) limun.org**

The title picture of this weblog shows the watch floor of the NSA's National Security Operations Center (NSOC) in 2006. The URL of this weblog recalls Electrospace Systems Inc., the company which made most of the top level communications equipment for the US Government. All information on this weblog is obtained from unclassified or publicly available sources.

QW5kIGZpbmFsbHksIHRoaXMgaXMgd2hhdCBhIHRleHQgbG9va3MgbGlrZSwgd2hbiBpdCdZIG9ubHkgZW5jb2RIZCB3aXRolHRoZSBzdGFuZGFyZCBBCYNINjQgc3lzdGVtLiBHdWVzcyBob3cgY29tcGxpY2F0ZWQgaXQgbXVzdCBIZSB3aGVuIGlEgcmVhbCBzdHJvbmcyWxnb3JpdGhtIHdhcyB1c2VklG==

**View
PDF**

- 1) Click the download button
- 2) This will take you to our web page
- 3) Download the FREE product



Download 

9/22/2014

Top Level Telecommunications: About STELLARWIND and other mysterious classification markings

[Post a Comment](#)

[Home](#)

[Older Post](#)

Subscribe to: [Post Comments \(Atom\)](#)

Awesome Inc. template. Powered by [Blogger](#).